International Journal of Computer Networking,
Wireless and Mobile Communications (IJCNWMC)
ISSN (P): 2250-1568; ISSN (E): 2278-9448
Vol. 7, Issue 4, Dec 2017, 11-18
© TJPRC Pvt. Ltd.

TRANS STELLAR
•Journal Publications •Research Consultancy

PERFORMANCE ANALYSIS OF SELECT FORWARDING ATTACK ON WSN AND ITS DETECTION AND REMOVAL FROM NETWORK

VIJETA KUMAWAT[1], KAVITA[2] & B. S. JANGRA[3]

[1]*Research Scholar, Department of Computer Science & Engineering, Jayoti Vidyapeeth Womens University, Jaipur, India*

[2]*Guide, Department of Computer Science & Engineering, Jayoti Vidyapeeth Womens University, Jaipur, India*

[3]*Co-Guide, Department of Computer Science & Engineering, FGM Govt. PG College, Hisar, India*

ABSTRACT

Wireless Sensor Networks is quite vulnerable to many security compromising attacks as wormhole attack, message replay or tampering, identity spoofing, black hole attack, eavesdropping, and so on. One of the impacts of select forwarding attack is that, it can be used to drops some of data packets. LEACHES (LowEnergy Adaptive Clustering Hierarchy) apply cluster rotation randomly for distribution of energy among all sensor nodes. In this paper, Selective Forwarding Attack creation, detection, and then removal are done on LEACH routing in Wireless Sensor Networks. It is an alyzed that how performance of networks affected with select forwarding attack then performance of detection & removal algorithm is analyzed. Moreover Performance of LEACH has been evaluated in terms of Packet Delivery Ratio with number of attacker node of select forwarding attack. The proposed analysisis simulated using network simulator NS2. The prevention technique is significantly successful in handling the attack, while restoring the performance of network and reduces the effect of attack from the network.

KEYWORDS: WSN, LEACH & Select Forwarding Attack

Received: Feb 23, 2017; **Accepted:** Mar 20, 2017; **Published:** Nov 24, 2017; **Paper Id.:** IJCNWMCDEC20172

Original Article

INTRODUCTION

A Network is a system of a network is a system of devices connected with each other for sharing information, resources and to communicate using protocols. With the vast and fast progress in wireless technology, there are various wireless networks are available which is classified into Infrastructure based and Infrastructure less networks. Wireless devices use oftenest or infrared signals for communication. MANET is consist of networking devices which are changes configuration according to its need, in this way each device works either as a router or a host in the network. Wireless networks have applications in personal, industrial personal and military [1]. Infrastructure less networking is known as Ad-hoc Networking which is classified into Wireless Mesh Networks (WMNs), Mobile Ad-hoc Networks (MANETs) and Wireless Sensor Networks (WSN) [2]. MANET is useful due to need of less infrastructure, easy installation, low cost bandwidth, low power consumption but network performance and security is a concern issue for researchers [3]. Each node of MANET is receiving and sending routing information and forwarding traffic on behalf of different nodes [4]. In Leach Routing, data is transferred to base station though cluster head [5]. Wireless Sensor Network is used to measure environmental data in remote location, process huge data and sends this to central location which is called Base Station. These WSN applications are very important useful requirement in collection of data from remote location where permanent structure is not possible as military applications, environmental condition detection, whether

predictions, humidity measurement etc. Each sensor node is operated using battery and hard difficult to replace or recharge battery in remote areas. Routing protocols should be energy efficient for Wireless Sensor Networks. This paper is identify the performances of LACH routing protocols for WSN Network on performance parameter such packet delivery ratio routing over energy level of battery and an effect select forwarding attack on simulation with NS-2 simulator. Moreover performance of detection algorithm of select forwarding attack is analyzed.

Wireless Sensor Networks Have following Characteristics

- Each Sensor node has limited memory and computation capabilities.
- Each Sensor nodes have limited battery and whenever battery is discharged below threshold level then sensor node is dead [5].
- Density of sensor nodes is more in WSN than MANET.

RELATED WORK

Different routing protocol are developed for WSN but Leach routing have avantage of efficient energy consumption. There are different attacks possible on leach routing as sink hole attack, worm hole attack and select forwarding attacks etc. Different detection techniques of malicious node are also developed for above attack [6] Ismail Butun et al. Have reviewed different possible intrusion detection techniques for WSN In [7]; an Intrusion detection technique is suggested basis of clustering but has à drawback of high consumption of energy. Leach is routing protocol which has characteristics of efficient energy consumption for WSN.

Leach Routing Low Energy Adaptive Clustering Hierarchy

In each cluster of sensor nodes, a node is elected as a local base station for fixed time duration and is elected as the cluster head for that particular cluster. Sensor node can send its sensor data to concern cluster head (CH) only. As, all the cluster members are communicating with a single node, that is, their cluster head, so, the cluster head needs more computation and transmission as compared to the member sensor nodes[8]. LEACH protocol uses cluster head rotation randomly among sensor nodes to avoid rapid dying of cluster head, so that energy of all the sensor nodes is consumed equally and enhances the overall alive-time of networks. Using local data fusion technique at each cluster head, compressed data is sent to the base station by each cluster head. Cluster head selection is based on energy probability distribution in which The CH nodes broadcast their status of being cluster head to all other sensor nodes in the sensor networks, so that each member node can know about the cluster head it belongs. TDMA schedule decides the communication pattern of the member nodes with their corresponding cluster head. All the sensor nodes keep their transmitter inactive all the time, except their transmitting time to save the energy of sensor nodes. After receiving data from all the remote member nodes, the cluster head performs data aggregation operations and send this aggregated data to the base station which requires high energy transmission from remote station sensor for data transfer [9, 10].

Select Forwarding Attack on Leach Routing [11, 12]

Let define the number of sensor nodes as N_i…….N_n and BS is base station. Let define Malicious_Node (MN) be the malicious node.

Repeat for every Sensor Nodes N_i …… $N_{n,}$

do

set threshold, $T(Ni) = \frac{Ei(t)}{Etotal} * k$

if (Random Number (Ni) ≤ T (Ni)) then

Node Ni is determined as a Cluster Head.

end if

end for

for each Cluster Head

do

for each node N_i to $N_{n,}$

do

Node N_i is a member of the cluster C_i based on distance from Cluster Head.

end for

end for

for each Cluster Group

do

If malicious node (MN) is selected as CH

then

for all member nodes n_i of this cluster, do

if(($n_i$mode 2) != 1) then

Send to base station after Aggregation on received data

else

drop received data from odd node.

end if

end for

else

for each m_i (member node) of this cluster

Process the received data and send to base station.

end for

end if

end for

PROPOSED WORK

It is hard to determine the optimal network under different Network scenario as traffic load with varying number of malicious node in network. WSN Network is simulated in NS2 with simulation parameter mentioned in table 1 and packet delivery ratio is evaluated for WSN network. Select forwarding attack mentioned in section 2.B is performed on above WSN network and PDR is evaluated. For reducing the effect of malicious network, the detection technique is performed which detect the malicious node in network and remove it from network. A flow chart of detection and removal algorithm is shown in figure 1.

Detection-RemovalAlgorithm of Select ForwardingAttack for Short Route Path

Suppose N isnumber of node in network and M is the number of Member nodes in particular cluster for a random round R. D is the number of received data on Cluster Head in same round R.

Step1: Start for every round R

do

for all Cluster Head in round R_i, do

Threshold (Cluster Head) = (D/MN)*100.

If threshold (Cluster Head) ≥ fixed limit

then

Cluster Head is malicious node in network

Remove this node out of network.

end if

end for

Repeat for next round R=R+1

end for

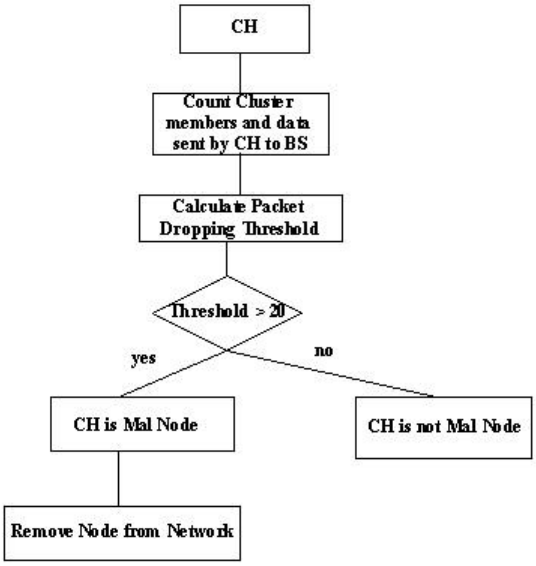

Figure 1: Detection and Removal of Attacknode in WSN

Table 1: Experimental Setup Simulation Parameters

Environmental Parameters	Value
Simulation Area	1000X1000 meter^2
Traffic Type in Network	Constant Bit Rate
Packet Size	1000 Bytes
Wi-Fi Type	IEEE 802.11 b
Routing Protocol	LEACH
Cluster Changing Time	20 msec
Simulation Time	100 Sec
Number of Sensor Nodes	100
Number of Advanced Nodes	10
Number of Normal Nodes	90
Energy of Advanced Nodes	4 Jules per node
Energy of Normal nodes	2 Jules per node
Expected Number of Clusters	5 clusters
Base Station Location	(60, 180)
Tool	NS2

EXPERIMENT RESULTS & ANALYSIS

Wireless Sensor Network is simulated in NS2 with simulation parameter mentioned in table 1 and packet delivery ratio evaluated with 3 different cases as without attack, with given select forwarding attack and with detection removal algorithm mentioned as proposed section. Packet Delivery Ratio: Packet Delivery Ratio (PDR) is metricused to measure the percentage of successfully delivered packets out of total number of sent packets. Experiments are performed on NS-2 simulator and calculated Packet Delivery Ratio over energy level for LEACH Routing and results are evaluated. The PDR was evaluated on number of malicious node and results are shown. PDR was evaluated with environment variable defined in Table 1 for without attack, with attack and after introducing Detection algorithm in Network as discussed in Section III [see table 2].

Table 2: Comparative Results of Select Forwarding Attack and Detection Technique

S No.	Scenario	PDR %
1	PDR without Select ForwardingAttack	100
2	Average PDR with Select Forwarding Attack	97%
3	PDR withDetectionAlgorithm	99%

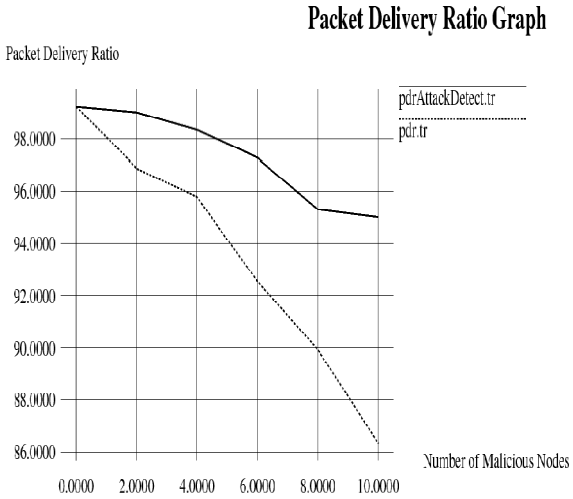

Figure 2: Comparative Results of Attack, Detection v/s Number of Malicious node

CONCLUSIONS

On the analysis of results of Table 2 and Figure 2, it is conclude that, select forwarding attack reduce the PDR and detection algorithm reduce the effect of select forwarding attack by detection of malicious node and subsequently remove malicious node from network. On increasing the malicious node in network, it reduces the PDR more. The PDR of network reduce up to 97 % on 2 malicious nodes in network but Detection algorithm increases 99%. The detection technique do not guarantee of achieving 100% PDR as detection takes some time duration and this time duration packets are dropped. The discussed detection technique of select forwarding attack can be modified and implemented with other routing protocol for WSN.

REFERENCES

1. *Pathan, Al-Sakib Khan, ed, "Security of self-organizing networks: MANET, WSN, WMN, VANET", CRC press, 2016.*
2. *Abosamra, A., Hashem, M., &Darwish, G.," Securing DSR with mobile agents in wireless ad hoc networks", Egyptian Informatics Journal, vol. 12, issue-1, pp. 29-36, 2011.*
3. *Dong, D., Li, M., Liu, Y., Li, X.-Y., & Liao, X.," Topological detection on wormholes in wireless ad hoc and sensor networks", IEEE/ACM Transactions on Networking(TON), Vol.-19, issue-6, pp. 1787-1796, 2011.*
4. *Kumari, Neelu, SandeepKumar Gupta, RajniChoudhary, and ShubhLaxshmiAgrwal. "New performance analysis of AODV, DSDV and OLSR routingprotocol for MANET." In Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on, pp. 33-35. IEEE, 2016.*
5. *Devadevan, V., and S. Suresh. "Energy Efficient Routing Protocol in Forest FireDetection System." In 2016 IEEE 6th*

International Conferenceon Advanced Computing (IACC), pp. 618-622. IEEE, 2016.

6. *Butun, Ismail, Salvatore D. Morgera, and Ravi Sankar. "A survey of intrusion detection systems in wireless sensor networks." Communications Surveys & Tutorials, IEEE 16.1 (2014): 266-282.*
7. *Jaiswal, Vibhuti PN, and Amit K. Garg. "An efficient protocol for reducing energy consumption in wireless sensor networks." Int. J. Eng. Res. Appl 2 (2012): 530-533.S*
8. *Razaque, Abdul, Musbah Abdulgader, Chaitrali Joshi, Fathi Amsaad, and Mrunal Chauhan. "P-LEACH: Energy efficient routing protocol for Wireless Sensor Networks." In 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), pp. 1-5. IEEE, 2016.*
9. *Singh, Takhellambam Sonamani, RanbirSoram, and AjoyKumar Khan. "Distance Based Multi Single Hop LowEnergy Adaptive Clustering Hierarchy (MS LEACH) Routing Protocol in Wireless Sensor Network." In2016 IEEE 6th International Conferenceon Advanced Computing (IACC), pp. 613-617. IEEE, 2016.*
10. *Shakya, Priyanka, Varun Sharma, and Anil Saroliya. "Enhanced multipath LEACH protocol for increasing network life time and minimizing overhead in MANET." In 2015 International Conference on Communication Networks (ICCN), pp. 148-154. IEEE, 2015.*
11. *Ren, Ju, Yaoxue Zhang, Kuan Zhang, and Xuemin Shen. "Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks." IEEE Transactions on Wireless Communications 15, no. 5 (2016): 3718-3731.*
12. *Khan, Wazir Zada, Yang Xiang, Mohammed Y. Aalsalem, and Quratulain Arshad. "The selective forwarding attack in sensor networks: Detections and counter measures." International Journal of Wireless and Microwave Technologies (IJWMT) 2, no. 2 (2012).*